UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
-v.-	:	17 Cr. 779 (KBF)
CHI PING PATRICK HO, a/k/a "Patrick C.P. Ho," a/k/a "He Zhiping,"	:	
Defendant.	:	

MEMORANDUM OF LAW OF THE UNITED STATES OF AMERICA
IN OPPOSITION TO THE DEFENDANT'S MOTION TO SUPPRESS

GEOFFREY S. BERMAN
United States Attorney
Southern District of New York

SANDRA MOSER
Acting Chief, Fraud Section
Criminal Division

Daniel C. Richenthal
Douglas S. Zolkind
Thomas McKay
Assistant United States Attorneys

David A. Last
Paul A. Hayden
Trial Attorneys

- Of Counsel -

TABLE OF CONTENTS

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
-v.-	:	17 Cr. 779 (KBF)
CHI PING PATRICK HO, a/k/a "Patrick C.P. Ho," a/k/a "He Zhiping,"	:	
Defendant.	:	

MEMORANDUM OF LAW OF THE UNITED STATES OF AMERICA IN OPPOSITION TO THE DEFENDANT'S MOTION TO SUPPRESS

The Government respectfully submits this memorandum of law in opposition to the motion of Chi Ping Patrick Ho, a/k/a "Patrick C.P. Ho," a/k/a "He Zhiping" (the "defendant") to suppress evidence from his Huawei cellphone and certain email accounts.

ARGUMENT

I. THE DEFENDANT'S MOTION TO SUPPRESS EVIDENCE OBTAINED FROM HIS CELLPHONE SHOULD BE DENIED

The defendant moves to suppress the results of a search warrant executed on one of his cellphones, claiming that the search is the fruit of a violation of the defendant's Fifth Amendment right not to incriminate himself.[1] But even assuming *arguendo* that the facts alleged by the defendant are true—though his claim about the agents' intent is not—his motion fails as a matter of law. The Supreme Court has squarely held that failure to give a suspect *Miranda* warnings does not require suppression of the physical fruits of the suspect's unwarned but

[1] The defendant appears only to move to suppress the results of the search of his Huawei cellphone, not any other electronic devices. (*See* Def. Br. 1.) Even if applied to other devices, however, his motion would be meritless for the reasons discussed herein.

voluntary statements.

A. Relevant Facts

On November 18, 2017, the defendant was arrested by special agents with the Federal Bureau of Investigation ("FBI") after his arrival at John F. Kennedy International Airport. Before the defendant was read his *Miranda* rights, an agent asked the defendant for the password to his iPad, so that the agent could put the iPad in airplane mode. The defendant told the agent his password, and the agent used the password to put the iPad in airplane mode and turn it off. The agent did not attempt to further access the iPad. When the agent began to ask the defendant the same questions with respect to his Huawei cell phone (the "Cellphone"), the defendant stated, in substance, that it had the same password as the iPad. The agent used that password to put the Cellphone into airplane mode and did not attempt to further access the Cellphone.[2]

On January 10, 2018, this Court signed a search warrant, authorizing law enforcement to review the contents of the iPad, the Cellphone, and several other electronic devices, all of which were seized from the defendant incident to his arrest (the lawfulness of which the defendant does not challenge). The FBI thereafter extracted the electronically stored information from the Cellphone, accessing it using the password provided by the defendant.

---

[2] The defendant asserts that the agents allegedly deliberately misled him, namely that they "asked [him] a question—under the guise of asking for a way to switch one device (iPad) into airplane mode—that was designed to elicit information (the Password) from [him]" in order to access another device (the Cellphone). (Def. Br. 7.) The Government expects that if an evidentiary hearing were ordered, the evidence would show that the request for the defendant's password was not the malevolent plot that the defendant invents. Rather, it is standard practice for law enforcement agents to attempt to place electronic devices into airplane mode so that they may not be remotely wiped, *i.e.*, to avoid a defendant destroying evidence before agents may lawfully execute a search warrant. This is a legitimate motivation that is entirely separate from any need to use a password to execute the search. Although the utility of having the password for any future search was not lost on the agents, they were also aware that a password is often not necessary to conduct a search. In any event, the Court need not—and therefore should not—order such a hearing, because the defendant's motion fails even assuming the truth of his hyperbolic version of the facts.

B. Applicable Law

In *Miranda v. Arizona*, 384 U.S. 436 (1966), the Supreme Court established certain procedural safeguards, commonly known as the *Miranda* warnings, which apply where an individual is subjected to custodial interrogation by law enforcement. Under *Miranda*, "the Fifth Amendment privilege against self-incrimination prohibits admitting statements given by a suspect during 'custodial interrogation' without a prior warning." *Illinois v. Perkins*, 496 U.S. 292, 296 (1990); *see also Dickerson v. United States*, 530 U.S. 428, 431-32 (2000) (*Miranda* held that "that certain warnings must be given before a suspect's statement made during custodial interrogation could be admitted in evidence").

As the Supreme Court has explained, *Miranda* warnings are a "prophylactic employed to protect against violation of the Self-Incrimination Clause." *United States v. Patane*, 542 U.S. 630, 636 (2004) (plurality opinion).[3] But the mere failure to provide *Miranda* warnings is not itself a violation of a defendant's rights: "Potential violations occur, if at all, *only* upon admission of unwarned statements into evidence *at trial*." *Id.* at 641 (emphasis added); *see also United States v. Verdugo-Urquidez*, 494 U.S. 259, 264 (1990) ("The privilege against self-incrimination guaranteed by the Fifth Amendment is a fundamental trial right of criminal defendants. Although conduct by law enforcement officials prior to trial may ultimately impair that right, a constitutional violation occurs only at trial." (citation omitted)). Thus, the Self-Incrimination Clause "is *not* implicated by the admission into evidence of the physical fruit of a voluntary statement." *Patane*, 542 U.S. at 636 (emphasis added). That is, "the exclusion of

[3] *Patane* was decided by a three-justice plurality opinion. Justices Kennedy and O'Connor concurred in the judgment, however, making a five-justice majority for the rule, discussed below, that "[a]dmission of nontestimonial physical fruits" of an unwarned statement "does not run the risk of admitting into trial an accused's coerced incriminating statements against himself." *Id.* at 645.

unwarned statements is a complete and sufficient remedy for any perceived *Miranda* violation," such that the "fruit of the poisonous tree" doctrine that applies in other contexts is inapplicable. *Id.* at 643.

C. Discussion

Patane forecloses the defendant's motion as a matter of law. For the purpose of this motion, the Court may assume both (a) that the defendant was in custody at the time the agents asked for his password, and (b) that the defendant had not yet been read *Miranda* warnings. The Government is not seeking to introduce the defendant's unwarned statements, *i.e.*, his provision of the password, in its case-in-chief, so there is no need to consider the defendant's motion to suppress his statement. But there is no basis in law to suppress the evidence on the Cellphone just because the password was used to expedite the search. *Patane* establishes a clear rule: The physical fruits of a voluntary unwarned statement are not subject to suppression. 542 U.S. at 634. The defendant has made no claim that his statement was *involuntary*, nor could he. That is conclusive. As this Court has previously recognized, "the Fifth Amendment's Self-Incrimination Clause 'cannot be violated by the introduction of nontestimonial evidence obtained as a result of voluntary statements.'" *Wilson v. Bradt*, No. 13 Civ. 6937 (KBF), 2014 WL 4116960, at *16 (S.D.N.Y. Aug. 20, 2014) (quoting *Patane*).

The cases cited by the defendant in arguing to the contrary are either inapposite or incorrect. The defendant cites an excerpt from *United States v. Crews*, 445 U.S. 463, 470 (1980), for the proposition that "the exclusionary sanction applies to any 'fruits' of a constitutional violation" (Def. Br. 8), but *Crews* was a Fourth Amendment case. As the Supreme Court explained in *Patane*, the fruits analysis applicable in that context does not apply here, because the prohibition against introducing an unwarned statement at trial "is a complete and sufficient remedy for any perceived *Miranda* violation." 542 U.S. at 643. The defendant's

citation to *United States v. Hubbell*, 530 U.S. 27, 38 (2000), is similarly inapposite. *Hubbell* is a statutory immunity case, and thus includes, by virtue of statute, a prohibition on use or derivative use of compelled statements. Plainly, no statute prohibits use of evidence obtained from a search of the defendant's Cellphone, which was searched pursuant to a search warrant.

The defendant primarily relies on *United States v. Djibo*, 151 F. Supp. 3d 297 (E.D.N.Y. 2015). (Def. Br. 9-10.) However, the district court in *Djibo* conflated the Fourth and Fifth Amendments in a manner that misapplied controlling precedent. The facts of *Djibo* are also very different from the facts here.

In *Djibo*, agents asked the defendant for the password to his cellphone at a moment when, in the district court's view, he was in custody but had not been advised of his *Miranda* rights. 151 F. Supp. 3d at 306-07. After the defendant gave the agents his password, the agents conducted a warrantless search of his phone, which the Government conceded was a Fourth Amendment violation. *Id.* at 307. After the agents later obtained a search warrant for the phone, the court found that the search pursuant to the warrant was the fruit of the illegal warrantless search. *Id.* at 309. Thus, unlike in this case, the search of the cellphone was the fruit of an earlier *Fourth* Amendment violation, such that fruit-of-the-poisonous-tree analysis was appropriate. Although that holding would have been sufficient to resolve the motion, the district court went on to discuss *Patane*. Without acknowledging the different doctrinal basis of *Patane*, the district court stated that it "declines to apply *Patane* to these facts for several reasons. As stated, *supra*, the Fourth Amendment protects individuals from unlawful searches and seizures." *Id.* at 309. The court went on to cite justifications—such as the volume of evidence on a cellphone—that sound in Fourth, not Fifth, Amendment doctrine. *See id.* at 310. Ultimately, the court held, the evidence obtained "by virtue of Djibo providing his passcode [is] suppressed as

either fruit of the unlawful inquiry by [the agent] after the [Customs] search ended, and/or fruit of the admittedly poisonous [warrantless search]." *Id.*

Simply put, *Djibo* was wrongly decided, because it failed to account for what *Patane* held about the Fifth Amendment's Self-Incrimination Clause. It is not violated when a suspect makes an unwarned statement. It is only violated when such an unwarned statement is introduced as evidence at trial. *Patane*, 542 U.S. at 641-42. For that reason, following *Patane*, the Second Circuit, this Court, and numerous other courts in this district have declined to apply fruit-of-the-poisonous-tree analysis to the physical fruit of a voluntary but unwarned statement. *See United States v. McCoy*, 407 F. App'x 514, 516 (2d Cir. 2010) ("The district court further concluded that because [the defendant's] statements that purportedly gave the officers consent to search were made before he was given *Miranda* warnings, the statements, in addition to the physical evidence discovered as a consequence of the statements, should be suppressed. This conclusion is foreclosed at least with respect to the physical evidence by the Supreme Court's decision in *United States v. Patane*, 542 U.S. 630[] (2004)."") (reversing order to suppress); *United States v. Haygood*, 157 F. App'x 448, 499 (2d Cir. 2005) ("[E]ven if defendant's statement of his address were necessary to provide a sufficient basis for a finding of probable cause, his challenge would nonetheless fall. The Supreme Court recently held in *United States v. Patane* . . . that the Self-Incrimination Clause of the Fifth Amendment cannot be violated by the introduction of nontestimonial evidence obtained as a result of voluntary statements." (internal quotation marks omitted)); *see also, e.g.*, *Bradt*, 2014 WL 4116960, at *16; *United States v. McDow*, 206 F. Supp. 3d 829, 848 n.13 (S.D.N.Y. 2016); *United States v. Fiseku*, No. 15 Cr. 384 (PAE), 2015 WL 7871038, at *16 (S.D.N.Y. Dec. 3, 2015); *United States v. Wilson*, 914 F. Supp. 2d 550, 558 & n.15 (S.D.N.Y. Dec. 18, 2012); *United States v. Alcantara*, No. 09 CR 231 (NRB), 2009 WL

4756491, at *11 (S.D.N.Y. Dec. 2, 2009).

The defendant nevertheless contends that applying *Patane* here would purportedly be "untenable" because of the volume and nature of material typically stored on a cellphone. (Def. Br. 10-11.) But the cases he cites for this proposition are Fourth Amendment cases, which apply that amendment's "reasonableness" inquiry. *See Riley v. California*, 134 S. Ct. 2473, 2482 (2014). There is no basis in law to engraft a Fourth Amendment concept onto the *Miranda* doctrine. *See, e.g.*, *Verdugo-Urquidez*, 494 U.S. at 264 (explaining different doctrinal bases for Fourth and Fifth Amendments). As discussed above, it is settled law that the "complete and sufficient remedy for any perceived *Miranda* violation" is exclusion of the statement itself. *Patane*, 542 U.S. at 643 (internal quotation marks omitted). Moreover, as the Supreme Court has explained, concerns about policy, like the one expressed by the defendant, must yield to the Constitution, which draws a distinction between a confessional statement and derived physical evidence. *Id.* at 643-44. With the exception of *Djibo*, courts have uniformly held that *Patane* forecloses the argument that the defendant makes, both generally, as described above, and specifically with respect to electronic devices. *See, e.g., United States v. Jackson*, Criminal No. 17-252 (DSD/FLN), 2018 U.S. Dist. LEXIS 55965, at *15-16 (D. Minn. Feb. 27, 2018) (magistrate report and recommendation); *United States v. Holland*, No. 15-CR-666-JMC, 2016 WL 6068020, at *4 (D.S.C. Oct. 17, 2016); *United States v. Stark*, No. 09-CR-20317, 2009 WL 3672103, at *3 (E.D. Mich. Nov. 2, 2009).

Finally, although the defendant does not actually make a *Franks* motion, *i.e.*, a motion based on an allegation of intentional and material misstatements or omissions in a search warrant, he suggests one by repeatedly noting that the affiant on the search warrant for the defendant's electronic devices did not state that agents had asked the defendant for his password

before he was read his *Miranda* rights. (Def. Br. 1, 3, 12). This suggestion is a red herring, with no apparent purpose other than to suggest misconduct when there was none, and the defendant is not entitled to suppression even if there was.

"A misstatement or omission is material if it is necessary to the issuing judge's probable cause finding." *United States v. Klump*, 536 F.3d 113, 119 (2d Cir. 2008). Put differently, an allegedly omitted fact is not material simply because it may have been of interest; it is material only if it would actually defeat probable cause. *E.g.*, *United States v. Salameh*, 152 F.3d 88, 113-14 (2d Cir. 1998); *Klump*, 536 F.3d at 120; *United States v. Levasseur*, 816 F.2d 37, 44 (2d Cir. 1987). This is so even where the omitted information is sufficiently important that the affiant "should have disclosed" it. *United States v. Bianco*, 998 F.2d 1112, 1126 (2d Cir. 1993) (although affiant "should have disclosed" fact that detracted from the Government's need for a roving Title III order, omission was not material because there would still be a basis for order).

The defendant does not acknowledge this requirement, and he cannot meet it. Whether the FBI had the passcode to the Cellphone and, if so, how it got it, was utterly irrelevant to the issue of whether there was probable cause to believe that the Cellphone contained evidence of federal criminal offenses. There either is a basis to believe that a cellphone or other electronic item has such evidence or there is not; whether the FBI has the passcode to the device adds absolutely nothing to that equation or the analysis of whether probable cause exists. There was no reason for the agent to include this irrelevant fact. Nor does the defendant offer a basis to conclude that the omission was part of a deliberate effort to mislead, rather than the result of a routine and appropriate decision not to include every possible detail, much less an irrelevant detail, in an affidavit. *See, e.g.*, *United States v. Awadallah*, 349 F.3d 42, 67-68 (2d Cir. 2003) ("the mere intent to exclude information is insufficient . . . [since] every decision not to include

certain information in the affidavit is 'intentional' insofar as it is made knowingly" (internal quotation marks omitted)). Nor would its inclusion have defeated probable cause. If anything, inclusion of the fact that the defendant gave the passcode to the phone would have *strengthened* the probable cause showing, by providing another piece of evidence that the phone belonged to the defendant.

Finally, even if there were merit to the defendant's motion—and there is none—the results of the search of the Cellphone would likely still be admissible pursuant to the independent source doctrine and/or inevitable discovery doctrine. That is so because for many electronic devices, a passcode is unnecessary, because the FBI's technicians can conduct the search regardless of whether they know the passcode. *See, e.g.*, *United States v. Ashmore*, 2016 U.S. Dist. LEXIS 185939, at *17 (W.D. Ark. Dec. 7, 2016); *see generally Nix v. Williams*, 467 U.S. 431, 444 (1984) ("If the prosecution can establish by a preponderance of the evidence that the information ultimately or inevitably would have been discovered by lawful means . . . then the deterrence rationale has so little basis that the evidence should be received."). The Court need not reach this issue (which in any event would require a fuller evidentiary record), however, because the defendant's motion fails as a matter of law under *Patane* and its progeny.

II. THE DEFENDANT'S MOTION TO SUPPRESS THE RESULTS OF EMAIL SEARCH WARRANTS SHOULD BE DENIED

The defendant also seeks suppression of the returns of search warrants executed on five email accounts used by him.[4] The defendant makes no challenge to the validity of the warrants themselves or the showing of probable cause that supported their issuance. Instead, he argues solely that the length of time it took the Government to complete its review of the voluminous returns from these warrants was so unreasonable as to violate the Constitution and mandate suppression. (Def. Br. 12.) The defendant is wrong. The Government's review of the returns of the email search warrants in question—which yielded hundreds of thousands of emails, including many in different languages—was eminently reasonable.

A. Relevant Facts

In the course of its lengthy investigation into the bribery and money laundering offenses with which the defendant is charged (the "Foreign Bribery Investigation")—which as the Court is aware, involves conduct in multiple countries across a multiple-year period—the Government has obtained search warrants on numerous different email accounts used by individuals involved in the Foreign Bribery Investigation. In total, the Government has obtained 31 search warrants relating to 19 different email accounts as part of the Foreign Bribery Investigation; 11 of these warrants relate to five different email accounts believed to be used by the defendant. These

[4] As an initial matter, the defendant has not submitted a sworn affidavit establishing that he has standing to challenge the search of the five email accounts he identifies as his own. If the defendant fails to do so in his reply, the Court can and should deny his motion on this ground alone. *See United States v. Montoya-Eschevarria*, 892 F. Supp. 104, 106 (S.D.N.Y. 1995). Moreover, in no event does the defendant have standing to move to suppress the results of search warrants executed on any of the *other* email accounts searched, which he does not contend belong to him, *see United States v. Villegas*, 899 F.2d 1324, 1333 (2d Cir. 1990), and he does not appear to seek suppression of these other warrants.

warrants were issued on or about June 16, 2016, August 4, 2016, October 24, 2016 and February 17, 2017,[5] and the returns of each of these warrants were typically provided to the Government by the service providers within a few weeks thereafter. (*See* Def. Ex. H, at 2.)

As the Government has informed the defendant, with respect to each of the defendant's accounts, a member of the prosecution team began reviewing the returns within approximately two weeks of receipt of them from the service providers. (*See id.*) That review included locating relevant and responsive documents, which were then cited in support of subsequent search warrants and ultimately the criminal complaint, as is evidenced by the search warrant affidavits and lengthy complaint.

All told, the returns of these warrants were extremely voluminous. They included more than 300,000 emails and attachments, more than 100,000 of which are associated with the accounts used by the defendant. More than a third of these emails and attachments are in Chinese, French, or another foreign language. Given the volume of data and the issues presented by the review of foreign-language documents, at great expense the Government retained a third-party vendor with the resources to help the Government more expeditiously sort the returns into materials "identified" as responsive to the relevant warrant(s) and materials "not identified" as responsive to the relevant warrant(s). The vendor worked under the direct supervision of the Government, pursuant to a detailed protocol. After a months-long, iterative process with the vendor, which included, among other things, developing and refining search terms, on March 23, 2018, the Government instructed the vendor to upload the set of "identified" materials relating to the Foreign Bribery Investigation to be processed and provided to the defendant in discovery. Thus, contrary to the defendant's suggestion (Def. Br. 12-13), as of March 23, 2018, the

[5] This last warrant is subject to a Rule 16(d) order authorizing delayed discovery.

Government has completed its review of the materials related to the Foreign Bribery Investigation obtained from the search warrants in question.[6] The Government has since segregated these materials in its online database and does not intend to further review the "non-identified" materials for evidence related to the Foreign Bribery Investigation.[7]

B. Applicable Law

"The touchstone of the Fourth Amendment is reasonableness." *United States v. Knights*, 534 U.S. 112, 118 (2001). Although the Government's execution of a valid search warrant is subject to reasonableness review, "searches pursuant to a warrant will rarely require any deep inquiry into reasonableness." *United States v. Ganias*, 824 F.3d 199, 209 (2d Cir. 2016) (en banc) (quoting *United States v. Leon*, 468 U.S. 897, 922 (1984)). Moreover, there is "no established upper limit as to when the government must review seized electronic data to determine whether evidence falls within the scope of a warrant." *United States v. Wey*, 256 F. Supp. 3d 355, 383 (S.D.N.Y. 2017) (citation omitted). Rather, numerous courts have held that "a delay of several months or even years between the seizure of electronic evidence and the completion of the government's review of it is reasonable." *United States v. Jarman*, 847 F.3d 259, 267 (5th Cir. 2017) (citation and alterations omitted). A case-specific analysis is required, because "computer searches are not, and cannot be subject to any rigid time limit because they

---

[6] There is one exception to this: During the Government's review of the search warrant returns, it realized that one production in response to one of the search warrants (not pertaining to one of the defendant's accounts) was incomplete. On or about March 22, 2018, the relevant service provider provided the Government with what it represents to be a complete production. On or about April 25, 2018, the Government and the vendor completed the process of identifying responsive materials from this later production.

[7] As noted above, one of the warrants in question is subject to a Rule 16(d) order. That warrant (as well as other warrants) authorize review of certain email accounts for evidence of other, as-yet-uncharged offenses. The Government has similarly engaged the third-party vendor to assist with this review, which is nearly complete.

may involve much more information than an ordinary search, more preparation and a greater degree of care in their execution." *United States v. Triumph Capital Grp.*, 211 F.R.D. 31, 66 (D. Conn. 2002).

C. Discussion

As discussed above, in the Foreign Bribery Investigation, the Government obtained more than 300,000 emails in response to 31 search warrants relating to 19 different email accounts. More than a third of these emails are in Chinese, French, or another foreign language. The warrants were issued over an eight-month period between June 2016 and February 2017. In each instance, the Government began reviewing the returns promptly upon the receipt and processing of the returns, and the evidence identified yielded probable cause for additional searches and, ultimately, a detailed criminal complaint. Cognizant of case law indicating that the Government should, after its initial review, make a final determination of which materials obtained pursuant to an electronic search warrant are responsive to the warrant, the Government retained a third-party vendor (at enormous financial expense) to assist in the extremely time-consuming task of sorting hundreds of thousands of emails in multiple languages into "identified" and "not identified" categories. The Government completed this process less than 12 months after it received all of the returns from the last series of search warrants relating to the defendant (*see* Def. Ex. H, at 2), and only four months after the defendant was indicted.[8]

[8] The defendant claims that it took the Government "[o]ver twenty-one months after it first began obtaining search warrants [*sic*] returns." (Def. Br. 12). As the defendant is aware from discovery, however, only a single search warrant for a single email account was issued in June 2016. The last search warrant returns for one of the defendant's accounts were received on or about March 25, 2017. (*See* Def. Ex. H, at 2.) In a case involving so many different email accounts and a series of search warrants following closely on the heels of one another, as well as related investigative steps, it was certainly reasonable for the Government to begin its review of each set of returns as those returns came in, but to wait until all the returns were in before retaining a third-party vendor and finalizing its identification of responsive documents. In any

This process was eminently reasonable. Indeed, as noted above, "numerous cases hold that a delay of several months or even years between the seizure of electronic evidence and the completion of the government's review is reasonable." *Jarman*, 847 F.3d at 267 (citation and alterations omitted). *See, e.g.*, *id.* at 266-67 (23 months was reasonable for review of seized hard drives where defendant was attorney and thus privilege review was necessary); *United States v. Lee*, No. 14-CR-227-TCB-2, 2015 WL 5667102, at *3-4 (N.D. Ga. Sept. 25, 2015) (denying motion to suppress where government had retained emails for more than three years without completing review); *United States v. Burns*, No. 07 Cr. 556, 2008 WL 4542990, at * 8-9 (N.D. Ill. Apr. 29, 2008) (ten months reasonable for search of a computer); *United States v. Gorrell*, 360 F. Supp. 2d 48, 55 n.5 (D.D.C. 2004) (ten months reasonable for search of two computers and storage drive). The Government's review process was more than reasonable here, where the warrants resulted in the return of hundreds of thousands of emails in multiple different languages.

None of the cases cited by the defendant suggests otherwise. Indeed, the defendant cites only a *single* case in which a court granted a motion to suppress based on the delay in reviewing electronic evidence (*see* Def. Br. 15 (citing *United States v. Metter*, 860 F. Supp. 2d 205 (E.D.N.Y. 2012)), but *Metter* is readily distinguishable. In *Metter*, the district court found a Fourth Amendment violation in an unusual case where, approximately 15 months after the government executed its search warrants, (a) the prosecution team identified "no plans whatsoever to *begin* review of that data" as required by the warrant and (b) the defendant had repeatedly sought return of the data belonging to him. 860 F. Supp. 2d at 211, 215 (emphasis in original). That is, *Metter* did not concern the length of time to *complete* the review of the

---

event, whether described as lasting 21 months or 12 months, the length of the Government's review was reasonable.

electronic evidence, but instead involved "[t]he government's retention of *all* imaged electronic devices, including personal emails, without *any* review whatsoever to determine not only their relevance to this case, but also to determine whether any recognized legal privileges attached to them." *Id.* at 215 (emphasis in original). Here, by significant contrast, the Government promptly began its review of the email returns within weeks of receipt of the returns from the service providers, and diligently completed its review and produced to the defendant those materials identified as responsive to the warrants. In addition, the defendant's first request for the return of property comes in a footnote in his brief in support of the instant motion, and in fact the Government already provided the defendant with complete copies of the search warrant returns for his accounts in discovery. (Def. Br. 16). This is a far cry from *Metter*.

The other cases cited by the defendant are even less persuasive. *United States v. Debbi*, 244 F. Supp. 2d 235, 237-38 (S.D.N.Y. 2003) (cited in Def. Br. 15), involved a search warrant for non-electronic evidence, in which the government repeatedly ignored requests by the defendant and even the court to identify and return non-responsive materials. The cited quotation from *Ganias* (*see* Def. Br. 15) is from a panel decision that was vacated by the *en banc* court, and describes not the government's delay in reviewing electronic evidence for responsiveness, but rather faults the government for its prolonged retention of documents that the government had *already determined* were not responsive to the search warrant. *See United States v. Ganias*, 755 F.3d 125, 137-38 (2d Cir. 2014). Finally, in *United States v. Wey*, 256 F. Supp. 3d 355 (S.D.N.Y. 2017), the district court held that the search warrants in question were facially deficient and that the resulting search could not be saved by the good faith exception. Nothing of the sort is even alleged to have occurred here. To be sure, in the course of the decision, the court criticized the repeated efforts of law enforcement to search data that had been

already identified as not responsive to the warrants but, notably, the court did *not* hold that such searches amounted to an independent Fourth Amendment violation, *see id.* at 405-06, and at no point did the court attempt to impose a specific time-limit on the government's ability to determine what electronic evidence was responsive to the warrant. None of these cases even remotely resembles this case, where the Government acted diligently to review the search warrant returns, identified the materials that were responsive to the search warrants, and thereafter created a segregated database to ensure that further review of materials obtained from the Foreign Bribery Investigation search warrants would *only* be done on materials identified as responsive.

Despite the fact that the defendant has not a single case that supports his argument, or even resembles this case, he asks for the remedy of "blanket suppression." But that remedy "should only be imposed in the most extraordinary of cases." *United States v. Shi Yan Liu*, 239 F.3d 138, 142 (2d Cir. 2000) (quoting *United States v. Foster*, 100 F.3d 846, 852 (10th Cir. 1996)). This is plainly not such a case. Absent some controlling precedent to the contrary—which the defendant has not identified, and of which the Government is unaware—the executing officers cannot be said to have acted in bad faith even if the Court determines, after the fact, that the timing of the search's execution was unreasonable. *See United States v. Clark*, 638 F.3d 89, 105 (2d Cir. 2011) (no bad faith absent controlling precedent); *United States v. Buck*, 813 F.2d 588, 593 (2d Cir. 1987) (same). The defendant is not entitled to the windfall that he seeks.

Finally, the defendant suggests without elaboration that the Court should hold a hearing if the Court feels that "additional information is necessary to rule on the present motion," such as "to [*sic*] extent to which the reviewers were assiduous in their review." (Def. Br. 17). But a defendant is not entitled to a hearing merely because he requests one. A hearing is warranted

only where "the moving papers are sufficiently definite, specific, detailed, and nonconjectural to enable the court to conclude that contested issues of fact" necessary to resolution of the motion are in question. *United States v. Pena*, 961 F.2d 333, 339 (2d Cir. 1992). The requirements that a defendant must meet to be entitled to a hearing exist for good reason, "[t]o avoid fishing expeditions." *United States v. Falso*, 544 F.3d 110, 125 (2d Cir. 2008). The defendant's request for a hearing is just that: Their challenge to the execution of the search warrants is self-evidently based on the length of time in which the review was conducted, but the defense has already been informed of the dates on which the Government received the returns of each search warrant relating to the defendant's accounts and the date on which the Government completed its identification of responsive emails (Def. Ex. H, at 2), and the defendant does not appear to dispute these facts. On the contrary, he embraces them. Nor does the defendant dispute the volume of the materials or the fact that they are in multiple languages. There is no material factual dispute, much less one that necessitates a hearing.[9]

[9] In a footnote, the defendant also purports to move for the return of his emails pursuant to Rule 41(g) (Def. Br. 17 n.5), but offers no justification whatsoever for his request. Nor is it clear what the defendant is seeking: As is relevant to his motion, the Government obtained no physical evidence from the defendant, but rather obtained electronic evidence from the service providers; the Government has *already* produced complete copies of these returns to the defendant; and the Government has segregated materials that are "not identified" into a separate database that it will not continue to review for evidence of the Foreign Bribery Investigation. This continued retention is likely necessary, *see Ganias*, 824 F.3d at 218-19, and absent something more than a conclusory footnote, the Court need not consider the defendant's Rule 41(g) motion further, *see United States v. Heatley*, No. 96 Cr. 515 (SS), 1997 WL 12961, at *2 (S.D.N.Y. Jan. 14, 1997) ("A footnote is not the proper place to raise a substantive argument.").

CONCLUSION

For the foregoing reasons, the defendant's motion to suppress should be denied.

Dated: New York, New York
May 15, 2018

Respectfully submitted,

GEOFFREY S. BERMAN
United States Attorney

By: s/ Douglas S. Zolkind
Daniel C. Richenthal
Douglas S. Zolkind
Thomas McKay
Assistant United States Attorneys
(212) 637-2109/2418/2267

SANDRA MOSER
Acting Chief, Fraud Section
Criminal Division

By: s/ David A. Last
David A. Last/Paul A. Hayden
Trial Attorneys
(202) 616-5651/353-9370